LISTING OF THE CLAIMS:

1. (Currently Amended) A method of operating a computer to read-in a password (*p*) upon a request of a program (E), the computer including an operating system having a generator module, the method comprising the steps of:

   the generator ~~modules~~ module of the operating system, receiving [a] an encrypted program-specific identifier (*H(E)*) from said program (E), and receiving said password;

   said generator module ~~generating from at least~~ using said encrypted program-specific identifier (*H(E)*) ~~and~~ to encrypt said received password (*p*) [a] to generate an encrypted program-password-specific identifier (*F(H(E),p)*); and

   sending said program-password specific identifier (*F(H(E),p)*) to said program (E), said program-password specific identifier (*F(H(E),p)*) being processable by said program (E) to authenticate said password.

2. (Previously Presented) Method according to claim 1, wherein

   - the program-specific identifier (*H(E)*) has been derived by applying a first cryptographic function (*H*) to at least part of the code of the program (E), and
   - the program-password-specific identifier (*F(H(E),p)*) is generated by applying a second cryptographic function (F) to the program-specific identifier (*H(E)*) and at least part of the received password (*p*), said first cryptographic function (*H*)

and/or said second cryptographic function (*F*) comprising a has function.

3. (Original) Method according to claim 1, wherein a password-reading program (26) and the program-specific identifier (*H(E)*) are provided by means of a trusted computing base (TCB), preferably for both the same trusted computing base (TCB).

4. (Original) Method according to claim 3, wherein the password (*p*) is received at the password-reading program (26), and, while said password-reading program (26) is executed, all I/O devices are locked and other programs are blocked.

5. (Original) Method according to claim 3, wherein the fact that the password-reading program (26) is executed based on the trusted computing base (TCB) is indicated via a signal, preferably illuminating an LED (28), while the password-reading program (26) receives the password (*p*).

6. (Original) Method according to claim 1, wherein the program-specific identifier (*F*(*H(E),p,s)*) is generated from the program-specific identifier (*H(E)*), the received password (*p*), and an additional value (s), said additional value (s) characterizing a device (2) where the program-password specific identifier (*F(H(E),p,s)*) is generated.

7. (Original) Method according to claim 1, wherein the program-specific identifier (*F(H(E),p)*) is used as a key to decrypt another program.

8. (Original) A computer program comprising program code means for performing the steps of claim 1 when said program is run on a computer.

9. (Original) A computer program product comprising program code means stored on a computer readable medium for performing the method of claim 1 when said program product is run on a computer.

10. (Currently Amended) A computer device (2) for reading-in a password (*p*) upon a request of a program (E) comprising:

an operating system including a generator module;

input means (14) for inputting said password (*p*);

receiver means (26) for receiving [a] an encrypted program-specific identifier (*H(E)*) from said program and said password (*p*) from a user; and

said generator-module (22) is connected to said receiver means (26) for receiving said password and said program-specific identifier and for ~~generating a program-password-specific identifier (*F(H(E),p)*) from at least said inputted password (*p*) and~~ using said encrypted program-specific identifier (*H(E)*) to encrypt said received password to generate an encrypted program-password-specific identifier, said program-password-specific identifier (*F(H(E),p)*) being processable by said program (E) to authenticate said password.

11. (Original) The computer device (2) according to claim 10, whereby the generator-module (22) is a has-function generator, and the program-specific identifier (*H(E)*) is derivable from the program (E) by use of said generator-module (22).

12. (Original) The computer device (2) according to claim 10, further comprising a trusted computing base (TCB) and indicator means (28) connected to this trusted computing base (TCB).

13. (Original) The computer device (2) according to claim 12, whereby the indicator means (28) provides a signal that indicates a secure entry mode while a password-reading program (26) provided by said trusted computing base (TCB) is executable.

14. (Currently Amended) A method according to claim 2, wherein said second cryptographic function is a one-way-~~has~~ hash function.

15. (Previously Presented) A computer system for reading in a password and generating an encrypted password in a secure manner, the computer system comprising:

a central processing unit (CPU);

a random access memory (RAM);

an input/output (I/O) interface including a password input device for receiving a user password from a user;

an operating system including a cryptographic-function generator module for creating program-specific identifiers and program-password-specific identifiers;

a password request program;

a password reading program;

an indicator means connected to the operating system to provide a signal indicating that the user password has been inputted;

wherein the operating system, the CPU, the RAM, and the I/O interface form a trusted computing base (TCB);

the password request program being connected to a commercial entity that that asks for entry of the user password, said commercial entity pre-storing a transformed password F [H(E), p];

the password request program receiving the inputted user password from the TCB;

upon receiving a request from the entity for the transformed password, the password request program forwarding said request to the password reading program;

the generator module generating a program-specific identifier H(E) and a program-password specific identifier;

the password request program sending a message to the password reading program, said message including the program–specific identifier H(E);

in response to receiving said message, the password reading program locks the I/O interface except for the password input device;

after the user password is received at the password reading program,

i) said locks are released,

ii) the generator module is applied to the program-specific identifier H(E) and the password p to generate a program-password specific identifier, and

iii) the generated program-password specific identifier is then sent from the password reading program to the password request program, and forwarded thereby to the commercial entity to verify that the generated program-password specific identifier is the same as said pre-stored transformed password F [H(E),p];

wherein the program-specific identifier (H(E)) is derived by applying a first cryptographic function (H) to at least part of the code of the password program request, and the generated program-password-specific identifier is generated by applying a second cryptographic function (F) to the program-specific identifier (H(E)) and at least part of the received password (p), said first cryptographic function (H) and said second cryptographic function (F) each comprising a hash function.

16. (Previously Presented) A computer system according to Claim 15, wherein only the TCB and the password reading program can control the indicator means, and said indicator means is a light emitting diode.